



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/808,260	03/23/2004	Michael D. Brent	010327-008600US	4180

20350 7590 02/08/2008  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER
----------

BAYOU, YONAS A

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

02/08/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

**Office Action Summary**

Application No.

10/808,260

Applicant(s)

BRENT, MICHAEL D.

Examiner

Yonas Bayou

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12/10/2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 March 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

1. This office action is in response to applicant's response filed on 12/10/2007.
2. Claims 1-21 are pending.
3. Applicant's arguments have been fully considered but they are not persuasive.
4. Examiner withdraws rejection of claim 1 under 35 U.S.C 112, second paragraph due to correction by the applicant.
5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

### Response to Arguments

1. Applicant, on page 7, line 28 – page 8, line 7, of the remarks, argues “Dotan does not teach storing a representation of configuration data associated with an operating system for the computer system obtained at a first time.”

Examiner respectfully disagrees and asserts that Dotan discloses that executable programs comprise a series of instructions that are executed by a central processing unit (CPU) of a computer system containing the program [see, **column 4, lines 17-20**; program corresponding to configuration data and a computer system corresponding to operating system].

2. Applicant, on page 8, lines 8-23, of the remarks, argues "Dotan does not teach comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time."

Examiner respectfully disagrees and asserts that Dotan discloses that the method of the present invention comprises comparing an initial state of an executable program to a final state of the program [see, **column 4, lines 21-22**].

3. Applicant, on page 9, lines 10-18, of the remarks, argues in the method of claim 7, which is rejected under 35 U.S.C 103(a) as being obvious over Dotan in view of Smith.

Examiner respectfully disagrees and asserts that Dotan does not appear to explicitly teach a method, wherein the stored representation of configuration data is encoded prior to being stored. However, Smith teaches that the email message may include an attachment that is encoded using MIME (Multipurpose Internet Mail Extension [**paragraph 82**]).

4. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Dotan, US Patent Number 5,822,517 (hereinafter Dotan).

Referring to claims 1, 19, 20 and 21, Dotan teaches a system, an article of manufacture and a method for detecting hostile software in a computer system comprising:

storing a representation of configuration data associated with an operating system for the computer system obtained at a first time **[column 4, lines 17-20]**;

comparing the stored representation of the configuration data obtained at the first time with a representation of the configuration data associated with the operating system for the computer system obtained at a second time **[column 4, lines 20-22]**;  
and

if deviation is detected between the stored representation of the configuration data obtained at the first time and the representation of the configuration data obtained

at the second time, automatically performing at least one remedial measure in response to the deviation detected **[column 4, lines 22-26]**.

Referring to claim 2, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data relates to identification of executable code installed in the computer system **[column 4, lines 17-20]**.

Referring to claim 3, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data relates to identification of a command line for invoking executable code associated with a particular file extension **[column 6, lines 4-9]**.

Referring to claim 4, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is obtained from a registry maintained by the operating system **[column 6, lines 1-7 and fig. 1]**.

Referring to claim 5, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data obtained from at least one key associated with the registry **[column 6, lines 1-7]**.

Referring to claim 6, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is obtained from a file stored in the computer system **[column 6, lines 1-7]**.

Referring to claim 8, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is compared to a predefined value **[column 4, lines 65-66, predefined value is corresponding to the state of the program]**.

Referring to claim 9, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is checked for addition of data **[column 6, lines 37-50, fig. 2A and fig. 2B]**.

Referring to claim 10, Dotan teaches a method for detecting hostile software in a computer system, wherein the configuration data is checked for removal of data **[column 4, lines 22-26, an alarm signal inform a user that the data has been modified (addition/removal) see fig. 2A and 2B]**.

Referring to claim 11, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises determining a storage location associated with suspected executable code in the computer system **[column 4, lines 57-64]**.

Referring to claim 12, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises determining whether suspected executable code is currently executing **[column 4, lines 51-56]**.

Referring to claim 13, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure further comprises terminating execution of the suspected executable code **[column 4, lines 57-64, restoring the infected program occurs by terminating execution of the suspected program]**.

Referring to claim 14, Dotan teaches a method for detecting hostile software in a computer system, wherein the suspected executable code does not receive notification prior to being terminated **[column 4, lines 51-56, prior to termination, the suspected executable program is being under the process of comparing initial state and final state]**.

Referring to claim 15, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises moving suspected executable code to a specified storage location for later evaluation **[column 4, lines 57-64]**.

Referring to claim 16, Dotan teaches a method for detecting hostile software in a computer system, wherein the at least one remedial measure comprises altering



configuration data associated with the operating system to reflect the stored representation of the configuration data **[column 5, lines 8-14]**.

Referring to claim 17, Dotan teaches a method for detecting hostile software in a computer system, wherein the operating system is a Windows-based operating system **[column 6, lines 9-12]**.

Referring to claim 18, Dotan teaches a method for detecting hostile software in a computer system, wherein the operating system is a Linux-based operating system **[column 6, lines 9-12, MS-DOS is corresponding to Linux-based operating system]**.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claim 7 is rejected under 35 U.S.C. 103(a) as being obvious over Dotan U.S. Patent Number 5,822,517 in view of Smith Pub. No. US 2002/0152399 A1.

Referring to claim 7, Dotan teaches a method for detecting hostile software in a computer system (see claim 1 above). Dotan further teaches storing a representation of configuration data associated with an operating system for the computer system obtained at a first time **[column 4, lines 17-20]**. Dotan does not appear to explicitly teach a method, wherein the stored representation of configuration data is encoded prior to being stored. However, Smith teaches that the email message may include an attachment that is encoded using MIME (Multipurpose Internet Mail Extension) **[paragraph 0082]**. Dotan and Smith are analogous art because both teach protection of software viruses.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to modify the method of Dotan to include an attachment that is encoded using MIME (Multipurpose Internet Mail Extension) **[paragraph 0082]** of Smith because the stored data is obtained in encoded form for scanning of virus protection purpose.

### ***Conclusion***

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f, 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.


Application/Control Number:  
10/808,260  
Art Unit: 2134

Page 10

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Yonas Bayou

02/6/2008

  
KAMBIZ ZAND  
SUPERVISORY PATENT EXAMINER